

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Streszczenie opinii EIOD w sprawie manipulacji online i danych osobowych

(Pełny tekst niniejszej opinii jest dostępny w wersji angielskiej, francuskiej i niemieckiej na stronie internetowej EIOD www.edps.europa.eu)

(2018/C 233/06)

Digitalizacja społeczeństwa i gospodarki ma mieszany wpływ na zaangażowanie obywateli w proces podejmowania decyzji oraz na bariery w zaangażowaniu społeczeństwa w procesy demokratyczne.

Analizy dużych zbiorów danych i systemy sztucznej inteligencji umożliwiły gromadzenie, łączenie, analizowanie i przechowywanie w nieskończoność ogromnych ilości danych. W ciągu ostatnich dwudziestu lat pojawił się dominujący model biznesowy dla większości usług internetowych, który polega na śledzeniu ludzi online i gromadzeniu danych na temat ich charakteru, zdrowia, relacji oraz myśli i opinii, mający na celu generowanie przychodów z reklam cyfrowych. Te rynki cyfrowe skupiły się wokół kilku przedsiębiorstw, które działają jako skuteczni strażnicy internetu i mają wyższe wartości kapitalizacji rynkowej skorygowane wskaźnikiem inflacji niż jakiegokolwiek inne przedsiębiorstwa w historii.

Ten cyfrowy ekosystem połączył ludzi na całym świecie – ponad 50 % populacji ma dostęp do internetu, choć pod względem geograficznym, bogactwa i płci jest on bardzo nierównomierny. Początkowy optymizm co do potencjału narzędzia internetowego i mediów społecznościowych w zakresie zaangażowania obywatelskiego ustąpił miejsca obawie, że ludźmi się manipuluje, po pierwsze poprzez ciągłe zbieranie często prywatnych informacji o nich, po drugie poprzez kontrolę nad informacjami, które widzą online, w zależności od kategorii, w jakiej są umieszczani. Wirusowe oburzenie w przypadku wielu usług opartych na algorytmach jest kluczowym czynnikiem wartości, ponieważ produkty i aplikacje są zaprojektowane w taki sposób, aby zmaksymalizować uwagę i uzależnienie. Połączenie, przynajmniej w obecnym modelu, doprowadziło do podziału.

Wynikająca z tego debata koncentrowała się wokół wprowadzających w błąd, fałszywych lub szkalujących informacji („treści”) podawanych ludziom z zamiarem wywarcia wpływu na dyskurs polityczny i wybory; zjawisko to określa się mianem „fałszywych informacji” lub „internetowej dezinformacji”. Rozwiązania skupiły się na środkach zapewniających przejrzystość, ujawniając źródło informacji, a jednocześnie zaniechując rozliczalność w ekosystemie tych podmiotów, które czerpią korzyści ze szkodliwych zachowań. Tymczasem koncentracja na rynku i wzrost dominacji platform stanowią nowe zagrożenie dla pluralizmu mediów. Zdaniem EIOD ten kryzys zaufania do ekosystemu cyfrowego ilustruje wzajemną zależność prywatności i wolności wypowiedzi. Zmniejszenie przestrzeni prywatnej dostępnej dla ludzi, będące wynikiem nieuniknionego nadzoru ze strony przedsiębiorstw i rządów, ma zniechęcający wpływ na zdolność i gotowość ludzi do swobodnego wyrażania siebie i nawiązywania relacji, w tym w sferze obywatelskiej, która jest tak istotna dla zdrowia demokracji. Niniejsza opinia dotyczy zatem sposobu wykorzystywania danych osobowych w celu mikroukierunkowania na osoby i grupy określonych treści, przedmiotowych podstawowych praw i wartości oraz odpowiednich przepisów prawnych służących łagodzeniu zagrożeń.

EIOD od kilku lat opowiada się za ściślejszą współpracą między organami ochrony danych a innymi organami regulacyjnymi w celu ochrony praw i interesów osób fizycznych w społeczeństwie cyfrowym, dlatego w 2017 r. uruchomiliśmy cyfrowy system wymiany informacji. Biorąc pod uwagę obawy, że kampanie polityczne mogą wykorzystywać przestrzeń cyfrową w celu obejścia obowiązujących przepisów⁽¹⁾, uważamy, że nadszedł czas, aby rozszerzyć tę współpracę na regulatorów wyborczych i audiowizualnych.

1. DLACZEGO PUBLIKUJEMY NINIEJSZĄ OPINIĘ

(i) Trwająca intensywna debata publiczna

Obecnie toczy się intensywna debata publiczna na temat wpływu dzisiejszego rozległego i złożonego ekosystemu informacji cyfrowej nie tylko na gospodarkę rynkową, ale również na gospodarkę polityczną oraz na temat wzajemnych oddziaływań środowiska politycznego z gospodarką. Główne platformy znajdują się w centrum tego ekosystemu, czerpiąc niewspółmierne korzyści z rozwoju reklamy cyfrowej, i zwiększają swoją względną władzę w miarę jej rozwoju. Dane osobowe są potrzebne do segmentacji, ukierunkowywania i dostosowywania wiadomości przekazywanych osobom fizycznym, ale większość reklamodawców nie wie, w jaki sposób takie decyzje są podejmowane, a większość osób fizycznych nie wie, w jaki sposób są one wykorzystywane. System nagradza sensacyjne i wirusowe treści i zasadniczo

⁽¹⁾ Zob. np. <http://www.independent.co.uk/news/uk/politics/election-2017-facebook-ads-marginal-seats-tories-labour-outdated-election-spending-rules-a7733131.html> [dostęp: 18.03.2018].

nie rozróżnia reklamodawców, czy to komercyjnych, czy politycznych. Odkrycia w zakresie tego, jak za pośrednictwem tego systemu propagowano umyślną dezinformację („falszywe informacje”), wywołały obawy, że integralność demokracji może być zagrożona. Systemy sztucznej inteligencji, których rynek również charakteryzuje się koncentracją, same w sobie opierają się na danych i – jeśli nie są kontrolowane – zwiększają oddalenie i brak rozliczalności przy podejmowaniu decyzji w tym środowisku.

(ii) Znaczenie prawa o ochronie danych i kampanii politycznych

Podstawowe prawa do prywatności i ochrony danych są bez wątpienia kluczowym czynnikiem w naprawie tej sytuacji, co czyni z tej kwestii strategiczny priorytet dla wszystkich niezależnych organów ochrony danych. W rezolucji z 2005 r. w sprawie wykorzystania danych osobowych do celów komunikacji politycznej organy regulacyjne ds. ochrony danych wyraziły kluczowe na całym świecie obawy dotyczące ochrony danych związane ze zwiększonym przetwarzaniem danych osobowych przez podmioty niekomercyjne. Odnosiło się to w szczególności do przetwarzania „danych wrażliwych związanych z rzeczywistymi lub domniemanymi przekonaniem lub działaniami moralnymi i politycznymi lub z działaniami związanymi z głosowaniem” oraz „inwazyjnego profilowania różnych osób, które są obecnie klasyfikowane – czasami nieprawidłowo lub na podstawie powierzchownego kontaktu – jako sympatycy, zwolennicy, wyznawcy lub strony”⁽¹⁾. W międzynarodowej rezolucji wezwano do bardziej rygorystycznego egzekwowania przepisów o ochronie danych dotyczących minimalizacji danych, przetwarzania zgodnego z prawem, zgody, przejrzystości, praw osób, których dane dotyczą, ograniczenia celu i bezpieczeństwa danych. Być może nadszedł czas na odnowienie tego wezwania.

Prawo Unii w zakresie ochrony danych i poufności komunikacji elektronicznej ma zastosowanie do gromadzenia danych, profilowania i mikroukierunkowania, a jego prawidłowe egzekwowanie powinno pomóc w zminimalizowaniu szkód wynikających z prób manipulowania jednostkami i grupami. Partie polityczne przetwarzające dane wyborcze w UE wchodzą w zakres przepisów ogólnego rozporządzenia o ochronie danych. Ogólne rozporządzenie o ochronie danych definiuje dane osobowe ujawniające opinie polityczne jako szczególne kategorie danych. Przetwarzanie takich danych jest zasadniczo zabronione, chyba że ma zastosowanie jedno z wymienionych wyłączeń. W kontekście kampanii politycznych szczególnie istotne są dwa poniższe wyłączenia, które zasługują na pełne przytoczenie:

- „d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
- e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą; [...].
- g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą”.

W motywie 56 preambuły wyjaśniono art. 9 ust. 2 lit. g): „Jeżeli w ramach działań związanych z wyborami funkcjonowanie systemu demokratycznego w państwie członkowskim wymaga zbierania przez partie polityczne danych osobowych dotyczących poglądów politycznych obywateli, można zezwolić na przetwarzanie tych danych z uwagi na względy interesu publicznego pod warunkiem ustanowienia odpowiednich zabezpieczeń”.

Kilka organów ochrony danych opracowało zasady lub wytyczne dotyczące przetwarzania danych do celów politycznych:

- W marcu 2014 r. włoski Urząd Ochrony Danych przyjął przepisy dotyczące przetwarzania danych osobowych przez partie polityczne. W przepisach podkreślono ogólny zakaz wykorzystywania danych osobowych udostępnianych publicznie w internecie, np. na portalach społecznościowych lub forach, do celów komunikacji politycznej, jeżeli dane te zostały zgromadzone do innych celów⁽²⁾.
- W listopadzie 2016 r. francuska Krajowa Komisja Ochrony Danych (CNIL) przedstawiła dodatkowe wytyczne do swoich zaleceń z 2012 r. w sprawie komunikacji politycznej, określając zasady przetwarzania danych osobowych na portalach społecznościowych. W szczególności CNIL podkreśliła, że agregowanie danych osobowych wyborców w celu sprofilowania i dotarcia do nich na portalach społecznościowych może być zgodne z prawem wyłącznie wtedy, gdy opiera się na zgodzie jako podstawie przetwarzania danych⁽³⁾.

⁽¹⁾ Rezolucja jest dostępna pod adresem <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Political-Communication.pdf> [dostęp: 18.03.2018].

⁽²⁾ <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267> „Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall’informativa per fini di propaganda elettorale” opublikowane w Dzienniku Urzędowym włoskiego Urzędu Ochrony Danych nr 71, 26.3.2014 [dok. sieciowy nr 3013267].

⁽³⁾ <https://www.cnil.fr/fr/communication-politique-queles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux> „Communication politique: quelles sont les règles pour l’utilisation des données issues des réseaux sociaux?” opublikowane przez Commission Nationale de l’informatique et des libertés (francuską Narodową Komisję ds. Informatyki i Wolności), 8.11.2016.

— W kwietniu 2017 r. brytyjskie Biuro Komisarza ds. Informacji (ang. Information Commissioner's Office – ICO) wydało zaktualizowane wytyczne dotyczące kampanii politycznych, które zawierały również wytyczne dotyczące wykorzystania analizy danych w kampaniach politycznych. ICO wyjaśniło, że kiedy organizacja polityczna zleca firmie trzeciej przeprowadzenie analizy, firma ta może być przetwarzającym dane, podczas gdy organizacja – administratorem danych. Aby przetwarzanie danych było zgodne z prawem, należy uwzględnić szczegółowe przepisy prawa o ochronie danych regulujące stosunek między administratorem a przetwarzającym⁽¹⁾.

Wytyczne krajowych organów ochrony danych mogą potencjalnie zapewnić dodatkową miarodajną interpretację przepisów dotyczących ochrony danych i prawa ochrony prywatności, które odpowiadają za różnice w organizacji krajowych systemów politycznych⁽²⁾.

(iii) Cel niniejszej opinii EIOD

Wizja EIOD ma pomóc UE dawać przykład w globalnym dialogu na temat ochrony danych i prywatności w erze cyfrowej, określając interdyscyplinarne rozwiązania polityczne dotyczące wyzwań związanych z technologią dużych zbiorów danych i rozwijając wymiar etyczny przetwarzania danych osobowych⁽³⁾. Wezwaliśmy do traktowania osoby, której dane dotyczą, „jak osobę fizyczną, a nie tylko jak konsumenta czy użytkownika” i zwróciliśmy uwagę na kwestie etyczne związane ze skutkami profilowania w oparciu o przewidywania i personalizacji określonej algorytmem⁽⁴⁾. Wezwaliśmy do odpowiedzialnego i zrównoważonego rozwoju społeczeństwa cyfrowego w oparciu o indywidualną kontrolę nad danymi osobowymi, które go dotyczą, inżynierię i rozliczalność uwzględniające prywatność oraz spójne egzekwowanie prawa⁽⁵⁾. Grupa doradcza ds. etyki Europejskiego Inspektora Ochrony Danych w swoim sprawozdaniu ze stycznia 2018 r. zauważyła, że „mikroukierunkowywanie agitacji wyborczej zmienia zasady wypowiedzi publicznej, ograniczając przestrzeń do debaty i wymiany pomysłów”, co „pilnie wymaga demokratycznej debaty na temat wykorzystywania danych do celów kampanii politycznych i podejmowania decyzji”⁽⁶⁾.

Kwestia wykorzystywania informacji i danych osobowych do manipulowania ludźmi i polityką wykracza oczywiście znacznie poza prawo do ochrony danych. Zindywidualizowane, mikroukierunkowane środowisko online tworzy „bańki filtrów”, w których ludzie są narażeni na więcej powtarzających się informacji i spotykają się z mniejszą liczbą opinii, co prowadzi do zwiększonej polaryzacji politycznej i ideologicznej⁽⁷⁾. Zwiększa to powszechność i perswazyjność fałszywych opowieści i spisków⁽⁸⁾. Badania sugerują, że manipulowanie kanałami informacyjnymi lub wynikami wyszukiwania może mieć wpływ na zachowania wyborcze⁽⁹⁾.

EIOD pragnie przyczynić się do tego, by przetwarzanie danych osobowych, zgodnie ze słowami ogólnego rozporządzenia o ochronie danych, służyło ludzkości, a nie odwrotnie⁽¹⁰⁾. Postęp technologiczny nie powinien być hamowany, ale

⁽¹⁾ https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf Biuro Komisarza ds. Informacji „Wytyczne dotyczące kampanii politycznych” [20170426].

⁽²⁾ Zgodnie z art. 57 ust. 1 lit. d) ogólnego rozporządzenia o ochronie danych „każdy organ nadzorczy na swoim terytorium [...] upowszechnia wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia”.

⁽³⁾ Zob. *Leading by Example: The EDPS Strategy 2015–2019* (Dawanie przykładu: Strategia EIOD na lata 2015–2019), s. 17. Naszym zdaniem „duże zbiory danych” odnoszą się do praktyki łączenia ogromnych ilości informacji pochodzących z różnych źródeł i analizowania ich, często przy użyciu samouczących się algorytmów w celu podejmowania decyzji. Jedną z największych wartości dużych zbiorów danych dla przedsiębiorstw i rządów pochodzi z monitorowania zachowań ludzkich, zarówno zbiorowych, jak i indywidualnych, i ma potencjał do przewidywania; Opinia EIOD 4/2015, „W kierunku nowej etyki cyfrowej: dane, godność i technologia”, 11.9.2015, s. 6.

⁽⁴⁾ Profile wykorzystywane w celu przewidywania zachowania ludzi stwarzają ryzyko stygmatyzacji, wzmocnienia istniejących stereotypów, segregacji społecznej i kulturowej oraz wyłączenia społecznego, a tego rodzaju „zbiorowa inteligencja” podważa indywidualne wybory i równość szans. Podobne „bańki filtrów” oraz „osobiste przestrzenie odbicia echa” mogłyby doprowadzić do stłamszenia kreatywności, innowacyjności oraz wolności wypowiedzi i zrzeszania się, które umożliwiły wcześniej rozkwit cyfrowych technologii; Opinia EIOD 4/2015, s. 13 (źródła pominięto).

⁽⁵⁾ Opinia EIOD 7/2015 „Sprostanie wyzwaniom związanym z dużymi zbiorami danych”, s. 9.

⁽⁶⁾ Raport grupy doradczej ds. etyki EIOD, styczeń 2018, s. 28.

⁽⁷⁾ Zob. np. *The Economist*, *How the World Was Trolled* (4–10 listopada 2017), tom 425, nr 9065, s. 21–24.

⁽⁸⁾ H. Allcott i M. Gentzkow, *Social Media and Fake News in the 2016 Election* (wiosna 2017). Stanford University, *Journal of Economic Perspectives*, tom 31, nr 2, s. 211–236. <https://web.stanford.edu/~gentzkow/research/fakenews.pdf>, s. 219.

⁽⁹⁾ W jednym z eksperymentów użytkownicy platform społecznościowych zostali poinformowani o tym, jak ich znajomi powiedzieli, że głosowali, co spowodowało statystycznie istotny wzrost liczby osób (0,14 % ludności w wieku uprawniającym do głosowania, czyli około 340 000 wyborców) głosujących w kongresowych śródkresowych wyborach w 2010 r.; H. Allcott i M. Gentzkow, *Social Media and Fake News in the 2016 Election* (wiosna 2017). Stanford University, *Journal of Economic Perspectives*, tom 31, nr 2, s. 211–236, s. 219). W innym badaniu naukowcy twierdzili, że różnice w wynikach wyszukiwania Google były w stanie zmienić preferencje wyborcze niezdecydowanych wyborców o 20 %; Zuiderveen Borgesius, F. & Trilling, D. & Möller, J. & Bodó, B. & de Vreese, C. & Helberger, N. (2016). Should we worry about filter bubbles?. *Internet Policy Review*, 5(1). DOI: 10.14763/2016.1.401, s. 9.

⁽¹⁰⁾ Motyw 4 preambuły rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwanego dalej ogólnym rozporządzeniem o ochronie danych.

raczej kierowany zgodnie z naszymi wartościami. Poszanowanie praw podstawowych, w tym prawa do ochrony danych, ma zasadnicze znaczenie dla zapewnienia uczciwości wyborów, zwłaszcza w obliczu zbliżających się wyborów do Parlamentu Europejskiego w 2019 r. ⁽¹⁾ Niniejsza opinia jest najnowszą z serii szeroko zakrojonego zaangażowania EIOD w kwestie tego, w jaki sposób należy stosować ochronę danych, aby zaradzić najpilniejszym problemom dotyczącym porządku publicznego. Opiera się ona na poprzednich pracach EIOD dotyczących technologii dużych zbiorów danych i etyki cyfrowej oraz na potrzebie koordynacji regulacji dotyczących konkurencji i uczciwych rynków ⁽²⁾. W pierwszej części opinii podsumowany zostanie proces, w wyniku którego dane osobowe napędzają oraz określają dominujący cykl cyfrowego śledzenia, mikroukierunkowywania i manipulacji. Następnie rozważona zostanie rola różnych podmiotów w ekosystemie informacji cyfrowych. W opinii wzięte zostaną pod uwagę prawa podstawowe, odpowiednie zasady ochrony danych i inne stosowne zobowiązania prawne. Na zakończenie EIOD podkreśli, że problem manipulacji online ulegnie raczej tylko pogorszeniu, że żadne pojedyncze podejście regulacyjne nie będzie wystarczające samo w sobie i że organy regulacyjne muszą w związku z tym pilnie współpracować w celu rozwiązania nie tylko problemów nadużyć lokalnych, ale również zakłóceń strukturalnych spowodowanych nadmierną koncentracją na rynku.

7. PODSUMOWANIE

Manipulacja online stanowi zagrożenie dla społeczeństwa, ponieważ bańki filtrów i społeczności otoczone murami utrudniają ludziom wzajemne zrozumienie i dzielenie się doświadczeniami. Osłabienie tego „kleju społecznego” może podważyć demokrację oraz inne podstawowe prawa i wolności. Manipulacja online jest również symptomem braku przejrzystości i rozliczalności w cyfrowym ekosystemie. Problem jest realny i pilny, a prawdopodobnie ulegnie pogłębieniu wraz z podłączeniem do internetu coraz większej liczby osób i rzeczy oraz wzrostem roli systemów sztucznej inteligencji. U podstaw problemu leży częściowo nieodpowiedzialne, nielegalne lub nieetyczne wykorzystywanie danych osobowych. Przejrzystość jest konieczna, ale niewystarczająca. Zarządzanie treścią może być konieczne, ale nie może naruszać praw podstawowych. Częścią rozwiązania jest zatem rygorystyczne egzekwowanie istniejących przepisów, zwłaszcza ogólnego rozporządzenia o ochronie danych, w połączeniu z innymi normami dotyczącymi wyborów i pluralizmu mediów.

W ramach wkładu w postępy w debacie wiosną 2019 r. EIOD zorganizuje warsztaty, podczas których krajowe organy regulacyjne w dziedzinie ochrony danych oraz prawa wyborczego i audiowizualnego będą w stanie zbadać te wzajemne zależności, omówić stojące przed nimi wyzwania i rozważyć możliwości wspólnych działań, z uwzględnieniem zbliżających się wyborów do Parlamentu Europejskiego.

W niniejszej opinii stwierdzono, że technologia i zachowanie na rynku wyrządzają szkodę w wyniku braku równowagi strukturalnej i występowania zakłóceń. Wezwaliśmy do dostosowania środków zachęty do innowacji. Do tej pory giganci i pionierzy technologii czerpali korzyści z działania w stosunkowo nieuregulowanym środowisku. Dotyczy to tradycyjnych gałęzi przemysłu i podstawowych pojęć właściwości miejscowej, suwerenności, a także norm społecznych, w tym demokracji. Wartości te zależą od mnogości głosów i zasadzie równowagi między stronami. Żaden pojedynczy podmiot ani sektor nie jest w stanie sam rozwiązać tego problemu. Ochrona danych stanowi część rozwiązania – być może większą, niż się spodziewano. Nie wystarczy polegać na dobrej woli ostatecznie nierozliczalnych podmiotów komercyjnych. Musimy teraz interweniować w celu bardziej sprawiedliwego rozpowszechniania korzyści płynących z digitalizacji.

Sporządzono w Brukseli dnia 19 marca 2018 r.

Giovanni BUTTARELLI

Europejski Inspektor Ochrony Danych

⁽¹⁾ Jak stwierdził Europejski Trybunał Praw Człowieka w sprawie Orlovskaya Iskra przeciwko Rosji: „Wolne wybory i wolność wypowiedzi, zwłaszcza wolność debaty politycznej, razem stanowią podstawę każdego systemu demokratycznego. Te dwa prawa są ze sobą powiązane i wzajemnie się wzmacniają: na przykład wolność wypowiedzi jest jednym z »warunków« niezbędnych do »zapewnienia swobody wyrażania opinii przez obywateli przy wyborze władzy ustawodawczej«. Z tego względu w okresie poprzedzającym wybory szczególnie ważne jest, aby umożliwić swobodny przepływ wszelkiego rodzaju opinii i informacji. W kontekście debat wyborczych szczególne znaczenie ma niezakłócone korzystanie przez kandydatów z wolności słowa” (w tekście pominięto źródła), pkt 110. <http://hudoc.echr.coe.int/eng?i=001-171525>.

⁽²⁾ 2014 – wstępna opinia „Prywatność i konkurencyjność w erze dużych zbiorów danych”; 2015 – opinia 4/2015 „W kierunku nowej etyki cyfrowej: dane, godność i technologia”; 2015 – opinia 7/2015 „Sprostanie wyzwaniom związanym z dużymi zbiorami danych: wezwanie do zapewnienia przejrzystości, kontroli użytkownika i ochrony danych już w fazie projektowania, a także rozliczalności”; 2016 – opinia 8/2016 EIOD w sprawie spójnego egzekwowania praw podstawowych w erze dużych zbiorów danych.